What is claimed is:

Sub a1

1. An apparatus comprising:

an interface to map a device via a bus to an address space of a chipset in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

a communication storage corresponding to the address space to allow the device to exchange security information with the at least one processor in the isolated execution mode in a remote attestation.

2. The apparatus of claim 1 wherein the security information includes at least one of a static public key and a static key certificate.

3. The apparatus of claim 2 wherein the interface comprises:

a decoder to decode the address space onto the bus so that an access to the chipset is passed to the device.

4. The apparatus of claim 3 wherein the device accesses a chipset storage via the address space.

5. The apparatus of claim 4 wherein the communication storage comprises:

a configuration storage to store device configuration information.

6. The apparatus of claim 5 wherein the communication storage further comprises:

a status register to store device status of the device;

a command register to store a device command for a command interface set; and

an input/output block (IOB) to store input and output data corresponding to the command.

7. The apparatus of claim 6 wherein the configuration storage comprises:

a public key storage to store the static public key;

a key certificate storage to store the static key certificate; and

an interface set storage to store an interface set identifier, the interface set identifier identifying a command interface set supported by the device.

8. The apparatus of claim 7 wherein the configuration storage further comprises:

a manufacturer identifier storage to store a manufacturer identifier; and

a revision storage to store a revision identifier.

9. The apparatus of claim 7 wherein the command interface set is an initialization set, the initialization set supporting a reset command and a connect command.

10. The apparatus of claim 7 wherein the command interface set is an attestation set, the attestation set performing at least one of a public key enumeration, a key certificate enumeration, and a signing operation.

11. The apparatus of claim 10 wherein the status register comprises:

a connection field to provide a connection status to indicate that the device is responsive to the connect command; and

an estimate field to provide an estimate of processing time for an operation specified in the command.

12. The apparatus of claim 11 wherein the status register further comprises:

a self-test field to indicate status of a self test in response to the reset command.

13. The apparatus of claim 10 wherein the public key enumeration enumerates an additional public key other than the static public key.

14. The apparatus of claim 10 wherein the key certificate enumeration enumerates an additional key certificate other than the static key certificate.

15. The apparatus of claim 10 wherein the sign operation generates a signature to attest validity of the secure environment using a private key provided by the chipset.

16. The apparatus of claim 15 wherein the signature corresponds to signing a chipset parameter.

17. The apparatus of claim 16 wherein the chipset parameter is one of a chipset isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

18. The apparatus of claim 17 wherein the chipset isolated nub loader hash and the chipset isolated hash log are stored in the chipset storage.

19. The apparatus of claim 18 wherein the software hash and the nonce are provided by a process nub.

20. The apparatus of claim 19 wherein the output data include the signature.

21. A method comprising:

mapping a device via a bus to an address space of a chipset in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

exchanging security information between the device and the at least one processor in the isolated execution mode in a remote attestation via a communication storage corresponding to the address space.

22. The method of claim 21 wherein the security information includes at least one of a static public key and a static key certificate.

23. The method of claim 22 wherein mapping comprises:

decoding the address space onto the bus so that an access to the chipset is passed to the device.

24. The method of claim 23 wherein the device accesses a chipset storage via the address space.

25. The method of claim 24 wherein exchanging comprises:

storing device configuration information in a configuration storage.

26. The method of claim 25 wherein exchanging further comprises:

storing device status of the device in a status register;

performing a device command corresponding to a command interface set to a command register; and

storing input and output data corresponding to the command in an input/output block (IOB).

27. The method of claim 26 wherein storing in the configuration storage comprises:

storing the static public key in a public key storage;

storing the static key certificate in a key certificate storage; and

storing an interface set identifier in an interface set storage, the interface set identifier identifying a command interface set supported by the device.

28. The method of claim 27 wherein storing in the configuration storage further comprises:

storing a manufacturer identifier in a manufacturer identifier storage; and

storing a revision identifier in a revision storage.

29. The method of claim 27 wherein performing the device command comprises performing a reset command and a connect command corresponding to an initialization set.

30. The method of claim 27 wherein performing the device command comprises performing at least one of a public key enumeration, a key certificate enumeration, and a signing operation, the public key enumeration, the key certificate enumeration, and the signing operation corresponding to an attestation set.

31. The method of claim 30 wherein storing the device status comprises:

providing a connection status to indicate that the device is responsive to the connect command; and

providing an estimate of processing time for an operation specified in the command.

32. The method of claim 31 wherein storing the device status further comprises:

indicating status of a self test in response to the reset command.

33. The method of claim 30 wherein performing the public key enumeration comprises enumerating an additional public key other than the static public key.

34. The method of claim 30 wherein performing the key certificate enumeration comprises enumerating an additional key certificate other than the static key certificate.

35. The method of claim 30 wherein performing the sign operation comprises generating a signature to attest validity of the secure environment using a private key provided by the chipset.

36. The method of claim 35 wherein the signature corresponds to signing a chipset parameter.

37. The method of claim 36 wherein the chipset parameter is one of a chipset isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

38. The method of claim 37 wherein the chipset isolated nub loader hash and the chipset isolated hash log are stored in the chipset storage.

39. The method of claim 38 wherein the software hash and the nonce are provided by a process nub.

40. The method of claim 39 wherein the output data include the signature.

41. A computer program product comprising:

a machine readable medium having program code embedded therein, the computer program product comprising:

computer readable program code for mapping a device via a bus to an address space of a chipset in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

computer readable program code for exchanging security information between the device and the at least one processor in the isolated execution mode in a remote attestation via a communication storage corresponding to the address space.

42. The computer program product of claim 41 wherein the security information includes at least one of a static public key and a static key certificate.

43. The computer program product of claim 42 wherein the computer readable program code for mapping comprises:

computer readable program code for decoding the address space onto the bus so that an access to the chipset is passed to the device.

44. The computer program product of claim 43 wherein the device accesses a chipset storage via the address space.

45. The computer program product of claim 44 wherein the computer readable program code for exchanging comprises:

computer readable program code for storing device configuration information in a configuration storage.

46. The computer program product of claim 45 wherein the computer readable program code for exchanging further comprises:

computer readable program code for storing device status of the device in a status register;

computer readable program code for performing a device command corresponding to a command interface set to a command register; and

computer readable program code for storing input and output data corresponding to the command in an input/output block (IOB).

47. The computer program product of claim 46 wherein the computer readable program code for storing in the configuration storage comprises:

computer readable program code for storing the static public key in a public key storage;

computer readable program code for storing the static key certificate in a key certificate storage; and

computer readable program code for storing an interface set identifier in an interface set storage, the interface set identifier identifying a command interface set supported by the device.

48. The computer program product of claim 47 wherein the computer readable program code for storing in the configuration storage further comprises:

computer readable program code for storing a manufacturer identifier in a manufacturer identifier storage; and

computer readable program code for storing a revision identifier in a revision storage.

49. The computer program product of claim 47 wherein the computer readable program code for performing the device command comprises performing a reset command and a connect command corresponding to an initialization set.

50. The computer program product of claim 47 wherein the computer readable program code for performing the device command comprises performing at least one of a public key enumeration, a key certificate enumeration, and a signing operation, the public key enumeration, the key certificate enumeration, and the signing operation corresponding to an attestation set.

51. The computer program product of claim 50 wherein the computer readable program code for storing the device status comprises:

computer readable program code for providing a connection status to indicate that the device is responsive to the connect command; and

computer readable program code for providing an estimate of processing time for an operation specified in the command.

52. The computer program product of claim 51 wherein the computer readable program code for storing the device status further comprises:

computer readable program code for indicating status of a self test in response to the reset command.

53. The computer program product of claim 50 wherein the computer readable program code for performing the public key enumeration comprises enumerating an additional public key other than the static public key.

54. The computer program product of claim 50 wherein the computer readable program code for performing the key certificate enumeration comprises enumerating an additional key certificate other than the static key certificate.

55. The computer program product of claim 50 wherein the computer readable program code for performing the sign operation comprises generating a signature to attest validity of the secure environment using a private key provided by the chipset.

56. The computer program product of claim 55 wherein the signature corresponds to signing a chipset parameter.

57. The computer program product of claim 56 wherein the chipset parameter is one of a chipset isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

58. The computer program product of claim 57 wherein the chipset isolated nub loader hash and the chipset isolated hash log are stored in the chipset storage.

59. The computer program product of claim 58 wherein the software hash and the nonce are provided by a process nub.

60. The computer program product of claim 59 wherein the output data include the signature.

61. A system comprising:

at least one processor operating in a secure environment, the at least one processor having one of a normal execution mode and an isolated execution mode;

a memory coupled to the at least one processor, the memory having an isolated memory area accessible to the at least one processor in the isolated execution mode; and

a chipset coupled to the at least one processor and the memory, the chipset having a circuit, the circuit comprising:

an interface to map a device via a bus to an address space of the chipset in the secure environment, and

a communication storage corresponding to the address space to allow the device to exchange security information with the at least one processor in the isolated execution mode in a remote attestation.

62. The system of claim 61 wherein the security information includes at least one of a static public key and a static key certificate.

63. The system of claim 62 wherein the interface comprises:

a decoder to decode the address space onto the bus so that an access to the chipset is passed to the device.

64. The system of claim 63 wherein the device accesses a chipset storage via the address space.

65. The system of claim 64 wherein the communication storage comprises:

a configuration storage to store device configuration information.

66. The system of claim 65 wherein the communication storage further comprises:

a status register to store device status of the device;

a command register to store a device command for a command interface set; and

an input/output block (IOB) to store input and output data corresponding to the command.

67. The system of claim 66 wherein the configuration storage comprises:

a public key storage to store the static public key;

a key certificate storage to store the static key certificate; and

an interface set storage to store an interface set identifier, the interface set identifier identifying a command interface set supported by the device.

68. The system of claim 67 wherein the configuration storage further comprises:

a manufacturer identifier storage to store a manufacturer identifier; and

a revision storage to store a revision identifier.

69. The system of claim 67 wherein the command interface set is an initialization set, the initialization set supporting a reset command and a connect command.

70. The system of claim 67 wherein the command interface set is an attestation set, the attestation set performing at least one of a public key enumeration, a key certificate enumeration, and a signing operation.

71. The system of claim 70 wherein the status register comprises:

a connection field to provide a connection status to indicate that the device is responsive to the connect command; and

an estimate field to provide an estimate of processing time for an operation specified in the command.

72. The system of claim 71 wherein the status register further comprises:

a self-test field to indicate status of a self test in response to the reset command.

73. The system of claim 70 wherein the public key enumeration enumerates an additional public key other than the static public key.

74. The system of claim 70 wherein the key certificate enumeration enumerates an additional key certificate other than the static key certificate.

75. The system of claim 70 wherein the sign operation generates a signature to attest validity of the secure environment using a private key provided by the chipset.

76. The system of claim 75 wherein the signature corresponds to signing a chipset parameter.

77. The system of claim 76 wherein the chipset parameter is one of a chipset isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

78. The system of claim 77 wherein the chipset isolated nub loader hash and the chipset isolated hash log are stored in the chipset storage.

79. The system of claim 78 wherein the software hash and the nonce are provided by a process nub.

80. The system of claim 79 wherein the output data include the signature.